# DIGITAL IMAGING METHOD AND APPARATUS FOR DETECTION OF DOCUMENT SECURITY MARKS

## CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to co-pending, co-assigned U.S. application Ser. No. 09/328,481 filed Jun. 9, 1999 for "Digital Imaging Method and Apparatus for Detection of Document Security Mars."

## BACKGROUND OF THE INVENTION

The present invention relates to the digital image processing arts. More particularly, the application relates to a method and apparatus for preventing or inhibiting effective reproduction of documents such as currency, checks, stock certificates, and any other printed document including a pre-defined security mark printed therein. The subject method and apparatus operate to effect a multi-step review of all digital image data acquired from a printed document to be reproduced for purposes of locating any potential security marks and further examining same for purposes of positively identifying a potential security mark as an actual security mark. If a mark is located and verified to be an authentic security mark, effective reproduction of the printed document will not be permitted and/or other security measures will be taken.

The proliferation of digital image processing systems, such as digital color copiers, that are able to make very high quality reproductions or "copies" of color documents at a low cost has led to use of these machines by criminals for reproduction of currency, checks, stock certificates, legal documents, and other printed documents not legally reproducible. Obviously, any reproductions of these documents are counterfeit and illegal. Unfortunately, there has heretofore not been found a method or apparatus for effectively and efficiently detecting the attempted reproduction of currency and the like so that the reproduction may be thwarted. Without an effective an efficient method/apparatus for detecting currency and other non-reproducible documents, criminals have often been able to produce counterfeit documents almost at will.

Many difficulties are presented during the attempted identification of a security mark in a printed document. The documents, such as currency, are often significantly worn. Also, the document may be placed in the reproduction apparatus at an irregular angle or location that renders detection of the security mark more difficult. Also, improper or erroneous detection of a security mark, and any resulting operations to prevent duplication of the document, are likely to upset and inconvenience those attempting to make legitimate reproductions. Accordingly, erroneous detection of a security mark in a document must be minimized.

Based upon the foregoing and other considerations, a need has been found for a new and improved digital imaging method and apparatus for detection of document security marks to prevent production of counterfeit documents. It has been deemed desirable to develop such a method and apparatus that perform this function in an effective and efficient manner, without intrusion into or interruption of legitimate document reproduction efforts.

## SUMMARY OF THE INVENTION

In accordance with the present invention, a new and improved digital imaging method and apparatus are provided for effective and efficient detection of document security marks to prevent counterfeiting of documents.



In accordance with a first aspect of the present invention, a method of digital image processing is provided. The method includes, for a printed document potentially including a security mark defined therein by a plurality of actual mark constituents each having a select color, size, and shape and having a select spatial arrangement relative to each other, scanning the document to obtain digital image data corresponding to the printed document, the digital image data defined in terms of a plurality of color input pixel values. The digital image data is processed to identify all portions representing potential constituents of a security mark. For each potential mark constituent represented by the digital image data, it is determined if the potential mark constituent, together with at least one other potential mark constituent represented by the digital image data, defines a potential security mark. For each potential security mark represented in the digital image data, it is determined if the potential security mark represents an actual security mark present in the printed document.

In accordance with another aspect of the present invention, a digital image processing method for preventing unauthorized reproduction of a printed document including a security mark defined in terms of a plurality of actual mark constituents having a select color, select dimensions and arranged in a select pattern relative to each other, includes scanning said printed document to derive color digital data representing the printed document, the color digital data defined in terms of a plurality of pixels each having a color value. All pixels of the color digital data having a color value representing a color at least approximating the select color of the plurality of actual mark constituents are identified. A binary map of the color digital data is constructed and defined in terms of "on" and "off" pixels, the "on" pixels corresponding to the identified pixels of the color digital data having color values at least approximating the select color of the plurality of actual mark constituents. The binary map is used to identify potential mark constituents defined by the "on" pixels and to identify at least one neighborhood of plural potential mark constituents together defining a potential security mark. The potential security mark is identified as an actual security mark if the potential mark constituents thereof are uniform relative to each other. If an actual security mark is identified, effective duplication of the printed document is prevented.

In accordance with still another aspect of the present invention, a method of processing digital image data representing a color printed document that includes a security mark for purposes of identifying the security mark represented in the digital image data includes processing the digital image data to identify all portions thereof defining a select color corresponding to the color of the security mark in the printed document. For each portion of the digital image data defining the select color, it is determined if the portion represents a potential constituent of a security mark in the printed document. The method further includes, for each potential security mark constituent identified in the digital image data, determining if the potential security mark constituent, together with at least one other potential security mark constituent, defines a potential security mark. The potential security mark constituents defining each potential security mark are compared to each other to determine if they are uniform in terms of color and size relative to each other. A potential security mark is identified as a security mark represented in the digital image data if the potential security mark constituents of the potential security mark are